RL-TR-97-21
Final Technical Report
June 1997

DISA WIRELESS E-MAIL TRIAL

MOTOROLA, INC.

Steven Haney

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

19970728 163

DTIC QUALITY INSPECTED 4

Rome Laboratory
Air Force Materiel Command
Rome, New York

This report has been reviewed by the Rome Laboratory Public Affairs Office (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

RL-TR-97-21 has been reviewed and is approved for publication.

APPROVED:

JOSEPH A. MANCINI
Project Engineer

FOR THE COMMANDER:

JOHN A. GRANIERO, Chief Scientist
Command, Control & Communications Directorate

If your address has changed or if you wish to be removed from the Rome Laboratory mailing list, or if the addressee is no longer employed by your organization, please notify RL/C3BA, 525 Brooks Road, Rome, NY 13441-4505. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1997	Final Sep 94 - Jul 96

4. TITLE AND SUBTITLE

DISA WIRELESS E-MAIL TRIAL

5. FUNDING NUMBERS

C - F30602-94-C-0291
PE - N/A
PR - R376
TA - 01
WU - 04

6. AUTHOR(S)

Steven Haney

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Motorola, Inc.
Government and Systems Technology Group
8201 E. McDowell Road
Scottsdale, AZ 85252

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Rome Laboratory/C3BA
525 Brooks Road
Rome, NY 13441-4505

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

RL-TR-97-21

11. SUPPLEMENTARY NOTES

Rome Laboratory Project Engineer: Joseph A. Mancini/C3BA/(315) 330-7130

12a. DISTRIBUTION AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Wireless e-mail techniques were investigated with the objective being remote e-mail access of a user/evaluation group of 25 persons. Private, non-cellular radio connection services were utilized including ARDIS wireless network and RAM mobile data network. Correspondingly unique wireless modems were obtained and mated to the PCMCIA slot of notebook computers in the user/evaluation population, consisting of InfoTac and Mobedem wireless modems for use with ARDIS and RAM, respectively. Initially Secret Agent encryption software was utilized for data security but later FORTEZZA PCMCIA-type encryption cards were used to provide security for e-mail data up to confidential level. Various e-mail software packages were installed in and demonstrated via the notebook computers. A local area network which could access, bidirectionally, both the RAM and ARDIS networks and thus e-mail from users in the field using both radio mail systems, was installed at DISA and connected via an X.25 network. Late arrivals of FORTEZZA cards, high radio mail service rates and e-mail software difficulties have caused this effort to fall short of attaining all objectives.

14. SUBJECT TERMS

Wireless Communications, E-Mail, Personal Communications Systems (PCS)

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Standard Form 298 (Rev. 2-89) (EG)
Prescribed by ANSI Std. 239.18
Designed using Perform Pro, WHS/DIOR, Oct 94

Table of Contents

ABSTRACT 5

DESCRIPTORS 5

1. SCOPE 6

1.1 Identification 6

1.2 ProjectOverview 6

1.3 Assumptions 6

2. TECHNICAL Overview 7

2.1 Objectives Met 7

2.2 Objectives Not Met 8

3. Conclusions 8

APPENDIX A: Hardware and Software Installation Procedures A-1

1. Overview A-1

2. Assumptions A-1

3. Component Identification A-1

3.1. Hardware Components A-1

3.1.1. FORTEZZA Encryption Card A-1

3.1.2. InfoTAC Wireless Modem A-1

3.1.3. Mobedem Wireless Modem A-1

3.1.4. PCMCIA Card Reader A-2

3.1.5. X.25 Communications Card A-2

3.2. Network Components A-2

3.2.1. ARDIS Wireless Network A-2

3.2.2. RAM Mobile Data Network A-2

3.2.3. Local Area Network A-2

3.3. Software Components A-2

3.3.1. Microsoft Mail / Microsoft Mail Remote A-2

3.3.2. ArmorMail for Microsoft Mail A-2

3.3.3. Lotus cc:Mail / cc:Mail Mobile A-3

3.3.4. AirMobile Wireless for Lotus cc:Mail Mobile A-3

3.3.5. ArmorMail for Lotus cc:Mail A-3

3.3.6. CardWizard Pro A-3

3.3.7. Additional Software A-3

3.4. PC System Requirements A-4

3.4.1. MS-DOS 6.2 and Microsoft Windows 3.1 ..... A-4

3.4.2. CardWizard Pro (PCMCIA Drivers) A-4
3.4.3. 3COM EtherLink III Network Adapter A-4
3.4.4. Lotus cc:Mail Mobile A-5
3.4.5. Microsoft Mail Remote A-5
3.4.6. Motorola Air Mobile A-5
3.4.7. Armor-Mail for cc:Mail A-5
3.4.8. Armor-Mail for MS-Mail A-6
4. Installation Procedures A-5
4.1 MS-DOS 6.2 and Microsoft Windows 3.1 ..... A-6
4.2. CardWizard Pro A-6
4.3. 3COM Ethernet Software A-7
4.4. Lotus cc:Mail Mobile A-7
4.5. Microsoft Mail Remote A-8
4.6. Motorola Air Mobile A-9
4.7. Armor-Mail for cc:Mail A-9
4.8. Armor-Mail for MS-Mail A-10
APPENDIX B: Secure Wireless E-mail User's Guide B-1
5. System Operation: B-1
6. Before Installing the Included Software: B-1
6.1 Hardware Requirements B-1
6.2 Software Requirements B-2
7. Air Time Service B-2
8. Hardware Configuration: B-2
9. Software Configuration: B-2
9.1 Lotus cc:Mail Mobile Version 2.2 ..... B-2
9.2 Motorola AirMobile Version 1.12 ..... B-2
9.3 LJL ArmorMail for cc:Mail Version TBD B-2
10. Running the Software: B-3
11. Composing a Signed or Encrypted Message: B-3
12. Receiving a Signed or Encrypted Message: B-3
Appendix C: Air Time Providers C-1
1. ARDIS C-1

2. RAM Mobile Data C-1
APPENDIX D: Test Procedures D-1
1. Testbed D-1
2. Testbed Layout D-2
3. System Set-Up D-2
3.1. Hardware and Software Installation D-2
3.2. Network Set-Up D-2
4. System Test Considerations D-3
4.1. Baseline Establishment D-3
4.1.1. Lotus cc:Mail D-3
4.1.2. Ardis and AirMobile Wireless for Lotus cc:Mail Mobile D-3
4.1.3. AirMobile X.25 Server D-4
4.1.4. Microsoft Mail D-4
4.1.5. Microsoft Mail Remote and Microsoft Mail External D-4
4.2. ArmorMail D-5
4.2.1. ArmorMail using Microsoft Mail D-5
4.2.2. ArmorMail using Microsoft Mail Remote D-5
4.2.3. ArmorMail using Lotus cc:Mail D-5
4.2.4. ArmorMail using Lotus cc:Mail Mobile D-6
5. Encryption Software Test Procedures D-6
6. System Test Procedures D-8
6.1. Unencrypted E-Mail Test Procedures D-8
6.2. Encrypted E-Mail Test Procedures D-11
APPENDIX E: Problem History of LJL ArmorMail Software for Lotus cc:Mail E-1

List of Figures

Figure 1 - Motorola Secure Wireless E-Mail Testbed D-1

List of Tables

Table 1. - FORTEZZA Card Functional Tests D-6
Table 2. - FORTEZZA PIN Number Tests D-7
Table 3. - FORTEZZA.DIR File Tests D-8
Table 4. - Certificate File Verification Tests D-10

Table 5. - CKLFILE Tests D-11
Table 6. - Miscellaneous Functional Tests D-11
Table 7. - Unencrypted E-Mail Test Matrix D-12
Table 8. - Unencrypted E-Mail Test Procedures D-13
Table 9. - Encrypted E-Mail Test Matrix D-15
Table 10. - Encrypted E-Mail Test Procedures D-15

DOCUMENT ABSTRACT AND ANALYSIS

COMPANY PROPRIETARY

TITLE: Secure Wireless E-Mail Study

AUTHOR: Steve Haney

DOCUMENT NO: 70361-9503, Final Report Calendar Year 1995

ABSTRACT

The DISA Wireless E-Mail Trial was funded to develop technology in the emerging field of e-mail security. The goal of the DISA Wireless E-Mail Trial is to exploit products such as the FORTEZZA PCMCIA card and the NSA-developed local authority workstation (LAW). These systems will be integrated into a system that can provide e-mail security for sensitive-but-unclassified data, with future enhancement possibilities for Type 1 applications.

DESCRIPTORS

TESSERA	E-Mail	CAPSTONE
FORTESSA	PCMCIA	

1. Scope

1.1. Identification

This document is the Final Report for the DISA Wireless E-Mail Trial for contract F30602-94-C-0291.

1.2. Project Overview

The DISA Wireless E-Mail Trial was to enhance the existing DISA infra-structure to meet DISA's needs for wireless mobile e-mail with Type 2 security. The technology used to accomplish this task was based upon integrating COTS wireless mobile products and currently available NSA approved Type 2 security products into the existing DISA LAN and its associated mobile users. The process used to accomplish this task was a development period at Motorola GSTG for integration of the two technologies, followed by a six month trial period at DISA. The trial period began after the installation of the new system components into the DISA LAN.

The project goals were:

- improved system performance
- improved user interface to secure e-mail
- a six month evaluation of the Second Generation DISA LAN
- DMS compatibility
- exploration of future enhancement possibilities

The performance of the system and the user interface were evaluated during the trial period. DMS compatibility was to be accomplished by the use of DMS compatible security products. Possible future enhancements were to be reported upon in a series of studies that will evaluate the application of other technologies to government LANs.

1.3. Assumptions

Motorola GSTG assumed the following.

- The DISA LAN uses IBM compatible PCs
- The DISA Laptops have PCMCIA card slots and associated software
- DISA servers shall support the X.25 links to ARDIS and RAM

2. Technical Overview

DISA's pre-trial LAN was the subject of a trial called the First Generation Trial. The targets of the First Generation Trial were twenty Lotus cc:Mail Mobile users and five mobile Microsoft Mail (MSMail) users who communicate with the DISA LAN over the RAM Mobile Data Network using Intel Wireless Modems. The cc:Mail mobile users were equipped with Secret Agent encryption software and homed to four cc:mail servers on the DISA LAN. The mobile MS Mail users were homed to one MS Mail server on the DISA LAN and do not have encryption capability.

The goal of the Second Generation Trial was to improve DISA's existing wireless e-mail setup by implementing the following changes.

- Increase the wireless capability of the cc:mail users by enabling them to read the entire mail input box.
- Replace the Secret Agent software on the cc:mail systems with FORTEZZA card security and improve the user's e-mail interface. The FORTEZZA card security solution will also be applied to the MS Mail users.
- Add the ARDIS Network, a wireless data network, to DISA's existing wireless data capability.
- Install X.25 connections to the DISA LAN for the ARDIS Network and the existing RAM Mobile Data Network.

2.1 Objectives Met

A majority of the planned testing has been completed. The original design of the encrypted e-mail system was based on the MailSurfer program by Complex Architectures, Inc. (CAI). Although it would support Microsoft Mail over wireless, the decision was made to replace that system with AirMobile, a product of the Motorola Wireless Data Group (see **Objectives Not Met**). The AirMobile software has been optimized for transmission in a wireless environment. In addition, the connection between the AirMobile server and the provider network is through an X.25 interface which provides high speed and reliability.

There are several encrypted e-mail communications methods that have been tested successfully. Among those are the following:

- Messages have been transmitted over wireless modems using cc:Mail Mobile and its post office.
- Messages have been transmitted over the TSCO LAN using Microsoft Mail.
- Attachments have been received and forwarded using both of the above methods.
- Large (> 100K) messages have been transferred using the wireless technology.

In addition to the wireless tests, the X.25 server connection to the RAM Mobile Data network has been installed and is being used for additional testing of encrypted traffic using AirMobile X.25 server software. So far this server connection has been proven to be reliable.

2.2 Objectives Not Met

Phase II of the integration was not completed since the DISA Wireless E-Mail Trial was an integration effort using COTS applications, and testing was dependent on scheduled availability of the COTS software. The ArmorMail software went through many changes, from using the Tessera card which is no longer supported by NSA, to the Fortezza card currently in use. In addition, although ArmorMail for MSMail was available for testing early in the 1995, a version for cc:Mail that would work reliably had been released just before the end of the trial.

Although the CAI MailSurfer program had more features than the currently used system, the software was not robust due to reliability problems and the company was promising more than they could deliver. Because of the lack of support from CAI the decision was made to replace that system with Motorola WDG's AirMobile. This change in vendors caused delays in completing a final integration of all components of the system.

Testing of the X.25 version of AirMobile's server software for Ardis had been delayed due to the high cost of X.25 service provided by Ardis.

3. Conclusion:

DISA is continuing to test secure wireless e-mail traffic using the remaining funds to acquire network access from RAM Mobile Data. The primary value added technology for this effort was in developing the Secure E-mail infra-structure that ties the pieces together. The objective of the 1995 DISA Wireless E-Mail Trial, to position Motorola as the premier Secure E-Mail integrator, has been met.

APPENDIX A: Hardware and Software Installation Procedures

1. Overview

The installation of hardware and software for the Secure Wireless E-Mail Study can be accomplished by following the procedures outlined below. The procedures include assumptions made for each network and installation platform, and detailed instructions for each type of mail system (MSMail or cc:Mail).

2. Assumptions

The following characteristics of the target network is assumed:

- The LAN uses IBM compatible PCs
- The Laptops have PCMCIA card slots and associated software
- The servers shall support the X.25 links to ARDIS or RAM

3. Component Identification

The sections below describes each hardware and software component that is to be installed, and defines the PC system requirements for installation.

3.1. Hardware Components

In addition to the PC platform required by each user, some additional hardware is integral to the completion of system testing, as follows.

3.1.1. FORTEZZA Encryption Card

The FORTEZZA encryption card is a CAPSTONE based Type 2 compliant FORTEZZA PCMCIA cards with a self-contained cryptographic system. The programmed cards are supplied by Spyrus to Motorola GSTG.

3.1.2. InfoTAC Wireless Modem

The Motorola InfoTAC modem is an external wireless modem that is attached to the laptop via a serial connection cable to the serial port of the PC. The InfoTAC modem is used to communicate with the ARDIS network.

3.1.3. Mobedem Wireless Modem

The Ericsson Mobidem modem is an external wireless modem that is attached to the laptop via a serial connection cable to the serial port of the PC. The Mobidem modem is used to communicate with the RAM Mobile Data network.

3.1.4. PCMCIA Card Reader

For those PCs that do not have internal PCMCIA card readers, Databook TMD650 ThinLine Drive PCMCIA card readers are used to interface with the FORTEZZA cards.

3.1.5. X.25 Communications Card

The Eicon X.25 S51 card provides a hardware interface between the server software and the X.25 communications network. Using an X.25 card for server communications increases throughput compared to a wireless or standard dialup modem solution.

3.2. Network Components

The following Network Service Providers are utilized during software and system testing. Communications tests over a particular provider are based on resource availability and are not based on provider service.

3.2.1. ARDIS Wireless Network

The ARDIS network is composed of X.25 and wireless connections to the e-mail post office via either a Motorola InfoTAC wireless modem or a dedicated X.25 leased line.

3.2.2. RAM Mobile Data Network

The RAM Mobile Data network is composed of X.25 and wireless connections to the e-mail post office via either an Ericsson Mobidem wireless modem or a dedicated X.25 leased line.

3.2.3. Local Area Network

The Local Area Network (LAN) will be used to support the wired secure e-mail testing just as it has supported the standard Microsoft Mail and cc:Mail systems.

3.3. Software Components

The following software products complete the secure e-mail system.

3.3.1. Microsoft Mail / Microsoft Mail Remote

The Microsoft Mail software package provides normal LAN-based e-mail functionality, such as forwarding and file attachments. The Microsoft Mail Remote package adds non-LAN functionality to the operation of standard e-mail. In addition to being capable of operating in a LAN-connected mode, it can be configured for a dialin connection mode.

3.3.2. ArmorMail for Microsoft Mail

The ARMOR-MAIL Add-On software provides an interface between the FORTEZZA card and Microsoft Mail and Microsoft Mail Remote. This software enables the user to send signed and/or encrypted mail to anyone included in the users local Directory Services file on his/her PC. Each user must have the public key for each mail peer in this file.

3.3.3. Lotus cc:Mail / cc:Mail Mobile

The Lotus cc:Mail software package provides normal LAN-based e-mail functionality, such as forwarding and file attachments. The cc:Mail Mobile package adds non-LAN functionality to the operation of standard e-mail. In addition to being capable of operating in a LAN-connected mode, it allows configuration for wireless, dialin, TCP/IP, and other connection modes. When used with either a Mobidem or InfoTAC modem, it is used in wireless mode.

3.3.4. AirMobile Wireless for Lotus cc:Mail Mobile

The AirMobile client software provides the interface between Lotus cc:Mail Mobile and the wireless modems on each client computer. The AirMobile X.25 server software provides the interface between the e-mail post office on the LAN and the X.25 card on the server PC, which in turn connects to either the ARDIS or RAM wireless network.

3.3.5. ArmorMail for Lotus cc:Mail

The ARMOR-MAIL Add-On software provides an interface between the FORTEZZA card and Lotus cc:Mail and cc:Mail Remote. This software enables the user to send signed and/or encrypted mail to anyone included in the users local Directory Services file on his/her PC. Each user must have the public key for each mail peer in this file.

3.3.6. CardWizard Pro

CardWizard Pro is a software package which includes Socket Services, a PCMCIA driver for the interface between the PC and the PCMCIA card reader, and automatic configuration software.

3.3.7. Additional Software

In addition to the above mentioned software, the FORTEZZA encryption cards require other software in order to function. These include TESS.SYS, a card interface for the FORTEZZA card itself. Also, if an external card reader is utilized, software drivers for that reader are also necessary. These drivers and card interface programs are utilized, but are not tested except with during encryption tests with the FORTEZZA card.

Other software that is utilized during testing but is not specifically tested includes Windows 3.1 and the MS-DOS operating system.

3.4. PC System Requirements

The overall requirements for the PC system are based on the total individual software components used in the system. The amount of hard disk space each program requires is cumulative, but the amount of RAM required is not. Each software package recommends 4 MB of RAM, but since the packages will be used concurrently, at lease 8 MB of RAM is recommended for the overall system.

The system requirement for each client is:

- An IBM microcomputer with an 80386-class or higher CPU
- MS-DOS 6.2
- Microsoft Windows 3.1 or 3.11
- 8 MB of RAM
- 50 MB or greater disk space

The individual components and their requirements are listed in the following sections:

3.4.1. MS-DOS 6.2 and Microsoft Windows 3.1

MS-DOS 6.2 and Microsoft Windows 3.1 require:

- 18.3 MB of disk space.
- 8 MB of RAM.

3.4.2. CardWizard Pro (PCMCIA Drivers)

CardWizard Pro requires:

- 4 MB of RAM.
- 5 MB of disk space

3.4.3. 3COM EtherLink III Network Adapter

3COM EtherLink III requires:

- Personal Computer Memory Card International Association (PCMCIA) Release 2.01, 16-bit Type II or Type III card slot
- DOS 3.1 or higher
- Access to network operating system
- PCMCIA Drivers (CardWizard)

3.4.4. Lotus cc:Mail Mobile

Lotus cc:Mail Mobile requires:

- IBM microcomputer with an 80386-class or higher CPU
- Microsoft Windows 3.1 or 3.11
- 4 MB of RAM
- 10 MB of available disk space

3.4.5. Microsoft Mail Remote

Microsoft Mail Remote requires:

- IBM microcomputer with an 80386-class or higher CPU
- Microsoft Windows 3.1 or 3.11
- 4 MB of RAM
- 4 MB of available hard drive space

3.4.6. Motorola Air Mobile

Motorola Air Mobile requires:

- IBM microcomputer with an 80386-class or higher CPU
- 4 MB of RAM
- 2 MB of available disk space
- Wireless network adapter (e.g., InfoTAC or Mobidem-like device)
- Wireless network service (e.g., ARDIS or RAM)
- Microsoft Windows 3.1 or 3.11
- Lotus cc:Mail Mobile for Windows Release 2

3.4.7. Armor-Mail for cc:Mail

Armor-Mail for cc:Mail requires:

- IBM microcomputer with an 80386-class or higher CPU
- Microsoft Windows 3.1 or 3.11
- 4 MB of RAM
- 4 MB of available hard drive space

3.4.8. Armor-Mail for MS-Mail

Armor-Mail for MS-Mail requires:

- IBM microcomputer with an 80386-class or higher CPU
- Microsoft Windows 3.1 or 3.11
- 4 MB of RAM
- 4 MB of available hard drive space

4. Installation Procedures

The following installation procedures are based on the assumption that the computer is an IBM compatible computer with a PCMCIA slot and a floppy labeled "a:".

4.1 MS-DOS 6.2 and Microsoft Windows 3.1

The installation of DOS 6.22 should follow the instructions listed in the accompanying documentation. The installation of Microsoft Windows should follow the "Express Setup" instructions listed in the Windows documentation. A summary of user actions is listed below.

1. Insert Windows Disk 1 into Drive A:
2. Type "a:" and press ENTER
3. Type "setup" and press ENTER
4. It will prompt for EXPRESS SETUP or CUSTOM SETUP. Select EXPRESS SETUP and press ENTER.
5. The system will prompt the user for the next disk with a message stating "Insert disk 2 in drive a: and press ENTER". The user should remove disk 1 from drive a: and insert disk 2 into drive a:. Then the user should press ENTER.
6. Repeat step 5 for disks 3 through 6.
7. The system will prompt for PRINTER information. There is no printer attached. Select "NO PRINTER" and press ENTER.
8. The system will prompt for the identification of EDIT.COM which is the MS DOS Editor. The system has the proper identification. The user should press ENTER.
9. The user should next select "SKIP TUTORIAL" and press ENTER. This should terminate the Windows installation.

4.2. CardWizard Pro

The installation of CardWizard Pro should follow SystemSoft installation procedures. Insert the CardWizard Installation Disk in the PC, and follow the Quick Install instructions in the CardWizard documentation.

4.3. 3COM Ethernet Software

The installation of the 3COM Ethernet should follow 3COM installation procedures. A summary of the user actions is listed below.

1. Insert the 3COM installation disk into drive a:
2. Type "a:" and press ENTER
3. Type INSTALL and press ENTER
4. The screen will have a message displaying the items necessary for the system to contain before the 3COM drivers can be installed. The user should press ENTER.
5. A menu will be displayed next. The user should select from the STANDARD INSTALLATION AND CONFIGURATION menu. The NETWORK DRIVERS selection should be made. Then press ENTER. This will result in another menu being displayed.
6. The INSTALL NOVELL NETWARE DRIVERS selection should be made. Then press ENTER.
7. The user should then select the AUTO CONFIGURE 3COM ADAPTER item. The user should then press ENTER.
8. The installation is complete, press ESC to exit.

4.4. Lotus cc:Mail Mobile

The installation of Lotus cc:Mail Mobile product should follow the standard setup procedures. A list of the user actions follows.

1. Insert disk 1 into drive a:
4. Type "a:\setup" from the command prompt.
3. Press ENTER to continue
4. The "Lotus cc:Mail Mobile for Windows Setup" message will be displayed. Press ENTER to continue.
5. The system will display the prompt "Insert diskette labeled Disk 2 into A:\". Remove diskette 1 from drive a:, insert diskette 2 into drive a:, and press ENTER.
6. The system will display the prompt "Insert diskette labeled Disk 3 into A:\". Remove diskette 2 from drive a:, insert diskette 3 into drive a:, and press ENTER.
7. The system will prompt the user to update the AUTOEXEC.BAT file. Select OK and press ENTER.
8. The system will notify the user that the system must be restarted before starting Louts cc:Mail Mobile.

4.5. Microsoft Mail Remote

The installation of Microsoft Mail Remote should follow the "Express Setup" procedures. A list of the user actions follows.

1. Insert disk 1 into drive a:
2. Type "a:\setup"
3. Press ENTER to continue
4. The system will prompt for "name" and "organization". Enter "Secure E-Mail" for the name and "Motorola" for the organization. Press ENTER when complete.
5. The system will prompt the user to verify that the name and organization are correct.

   Press ENTER to continue.
6. The system will prompt for setup type. Select "Express Setup" and press ENTER to continue.
7. The system will prompt for approval of the C:\MSMAIL directory. Press ENTER to continue.
8. The system will prompt for approval to create the C:\MSMAIL directory (if it does not exist). Press ENTER to continue.
9. The system will prompt for approval to modify the AUTOEXEC.BAT file to include SHARE. Select YES and press ENTER.
10. The system will then prompt for disk 2. Remove disk 1 from drive a: and insert disk 2 into drive a:. Press ENTER to continue.
11. The system will prompt for disk 3. Remove disk 2 from drive a: and insert disk 3 into drive a:. Press ENTER to continue.
12. The system will prompt for the database disk. The default is "a:", which is correct. Remove disk 3 from drive a:, insert disk 4 which contains the database into drive a:, and press ENTER to continue.
13. The system will prompt for user action. Select EXIT and press ENTER.

4.6. Motorola Air Mobile

4.5 The installation of Motorola Air Mobile software is performed from Windows. The user should perform the following actions.

1. Insert the Air Mobile disk into drive a:
2. Click on the MAIN icon.
3. Click on the FILE MANAGER icon.
4. Click on the a: drive
5. Double click on the setup.exe file
6. The system will prompt for the c:\ccmobile directory. Press ENTER to accept this as the default directory.
7. The next message indicates that the installation is complete. Press ENTER to exit the setup program.

4.7. Armor-Mail for cc:Mail

The installation of Armor-Mail for cc:Mail software is performed from Windows. The user should perform the following actions.

1. Insert the Armor-Mail disk into drive a:.
2. In the Program Manager window, choose Run form the "File" menu. Type "a:\install" and press OK.
3. Select the destination directory from the dialog box.
4. Select the installation options listed in the Installation Options dialog box. The options are:

   Force Encryption when using MS-MAIL This eliminates the ability to bypass the Encryption/Decryption functionality of Armor-Mail.

   Copy Certificate Tree from floppy disk. This is used if you have a floppy disk with a PMSP directory structure containing the certificate tree.
5. The system will prompt for you to have the PCMCIA Driver supplied with the installation program installed. Select "No".
6. Select OK from the final dialog box, "Successful Installation".

4.8. Armor-Mail for MS-Mail

The installation of Armor-Mail for MS-Mail software is performed from Windows. The user should perform the following actions.

1. Insert the Armor-Mail disk into drive a:.
2. In the Program Manager window, choose Run form the "File" menu. Type "a:\install" and press OK.
3. Select the destination directory from the dialog box.
4. Select the installation options listed in the Installation Options dialog box.

   The options are:

   Force Encryption when using cc:Mail This eliminates the ability to bypass the Encryption/Decryption functionality of Armor-Mail.

   Copy Certificate Tree from floppy disk. This is used if you have a floppy disk with a PMSP directory structure containing the certificate tree.
5. The system will prompt for you to have the PCMCIA Driver supplied with the

   installation program installed. Select "No".
6. Select OK from the final dialog box, "Successful Installation".

This completes the software installation.

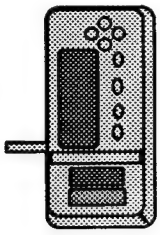
APPENDIX B: Secure Wireless E-mail User's Guide

This is the user's guide to the Secure Wireless E-mail System, a step-by-step procedure for using the software packages. This guide supplements the instructions supplied with the included software packages.

5. System Operation:

This system was designed to provide wireless e-mail security by encrypting messages and attachments before the messages are sent over a radio network. The security is provided by the FORTEZZA PCMCIA card, a Type-II encryption device. Messages are sent over a wireless network, provided either by Ardis or by RAM Mobile Data, using Motorola InfoTAC wireless modems.

FORTEZZA Encryption Card



InfoTAC Modem

The system also includes Motorola AirMobile software for communicating with the wireless network, Lotus cc:Mail e-mail software, and LJL ArmorMail encryption software which is used to interface with the FORTEZZA card to provide encryption.

6. Before Installing the Included Software:

You should verify that you have the following hardware and that the software described below has been installed on the target computer before installing the included software. Then install the included software per the instructions in the Software Installation Guide.

6.1 Hardware Requirements

- An IBM 386 or 486 PC or compatible and 8 Megs of RAM. The PC should also have either an external PCMCIA card reader or at least one internal PCMCIA card slot.
- A FORTEZZA PCMCIA encryption card.

6.2 Software Requirements

This software requires MS-DOS version 5.0 or greater, and Microsoft Windows version 3.1 or greater. If you are using an external PCMCIA card reader then use the drivers supplied with the card reader. If you are using an internal PCMCIA card slot, you should have SystemSoft's Card Services drivers installed.

7. Air Time Service

The InfoTAC wireless modem and communications software included in this package require an air time agreement with Ardis or RAM Mobile Data. Air time provider contact phone numbers are listed in Appendix C. This should be completed before attempting e-mail communication via the modem. However, the setup procedures may be followed before the air time agreement is in place.

8. Hardware Configuration:

- The FORTEZZA card should be inserted in the PCMCIA slot before powering up the computer. When the computer is booting up, the drivers will be installed and the card will be detected.
- Connect the InfoTAC wireless modem to the serial port with the supplied cable. Extend the antenna and turn on the modem. Refer to the InfoTAC User's Guide for the modem's configuration. The modem settings should be as follows:

Mode: Native

Startup: Native

- Power up the computer. When the command prompt is displayed, start Windows.

9. Software Configuration:

9.1 Lotus cc:Mail Mobile Version 2.2

- Follow the installation instructions in the Lotus cc:Mail Mobile "Getting Started Guide", using the procedures in the section, "Installing and Configuring cc:Mail Mobile for Windows, Logging in to cc:Mail Mobile for the First Time, Mobile Mode."
- For communication method type, select "Wireless." Be careful to specify the COM port to which the wireless modem is connected. Once this section has been completed, go on to the Motorola AirMobile instructions.

9.2 Motorola AirMobile Version 1.12

- Follow the instructions in the Motorola AirMobile Communication Client Guide for setup. The guide also includes additional instructions for setting up the cc:Mail software for use with AirMobile and a wireless modem.

9.3 LJL ArmorMail for cc:Mail Version TBD

- Install the certificate and CKL files per the instructions in the LJL ArmorMail User's Guide.

10. Running the Software:

- Make sure that the wireless modem is turned on.
- Double-click on the "Armorized cc:Mail" icon. This will bring up a requester for entering your password. Your name and post office directory should already be displayed in the requester.
- Enter the password and press ENTER. This will start the ArmorMail, cc:Mail, and AirMobile software packages. The ArmorMail software will then put up a requester for you to enter the PIN number for the your FORTEZZA card.
- Enter the PIN number and presses ENTER. The AirMobile software will then communicate with the wireless server using the InfoTAC modem. Any outgoing or incoming messages will be transmitted or received, as specified by the configuration you selected from within the cc:Mail software.

11. Composing a Signed or Encrypted Message:

Follow the instructions in the LJL ArmorMail User's Guide for instructions on creating and sending signed or encrypted messages.

12. Receiving a Signed or Encrypted Message:

Follow the instructions in the LJL ArmorMail User's Guide for instructions on reading signed or encrypted messages.

Appendix C: Air Time Providers

1. ARDIS

300 Knightsbridge Parkway
Lincolnshire, IL 60069
(708) 913 1215
(708) 913 1453 (FAX)

2. RAM Mobile Data

8100 Boone Blvd.
Suite 400
Vienna, VA 22182-2642
(703) 448-3839 (FAX)
(703) 448-3945

APPENDIX D: Test Procedures

1. Testbed

The secure wireless testbed is used for verifying operation and integrity of the encryption and wireless software. The testbed was created by integrating hardware and software components from the wireless and security products. The purpose and system interfaces of these add-on products are described in detail in succeeding sections. The diagram below describes the architecture of the network for testing the secure wireless e-mail system.

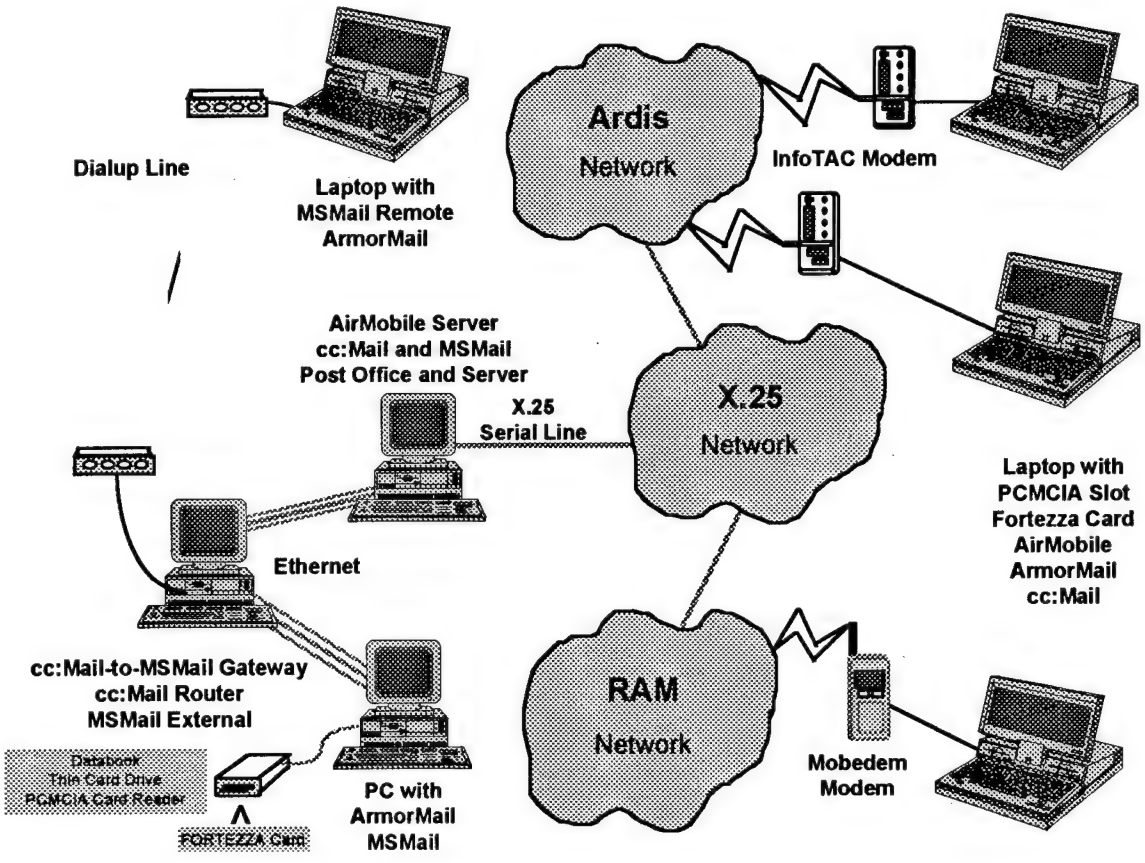


Figure 1 - Motorola Secure Wireless E-Mail Testbed

2. Testbed Layout

In order to fully exercise the software and encryption functions under test, a variety of laptop computers are used, including the AST PowerExec Notebook Computers. The AST PowerExecs have PCMCIA capability enabling the use of a FORTEZZA card for e-mail security. The other laptops have PCMCIA capability or have external card readers attached. Each has security software installed which allows the e-mail software on the Laptops to interact with the FORTEZZA card. Each Laptop is equipped with a radio modem to access one of the designated radio networks. Each component is described more fully in Appendix A, "Hardware and Software Installation Procedures".

3. System Set-Up

Before any software or system testing can be performed, all hardware and software must be installed on the target platforms and configured as required for the network. The network must also be configured to accommodate the required tests.

3.1. Hardware and Software Installation

Refer to Appendix A, "Hardware and Software Installation Procedures", for procedures on installing hardware and software to be used for system testing.

3.2. Network Set-Up

The network that is to support the secure e-mail testing should be configured ahead of time by the network administrator to support standard unencrypted e-mail for Microsoft Mail and cc:Mail.

4. System Test Considerations

There are a number of factors that are considered when system testing software that is developed as an addition/enhancement to an existing product. The integration of that new software into the existing system should take into consideration the following:

- Existing functionality of the original software should be maintained, except where the existing functions are fully replaced by the enhancement software.
- Added functionality or enhancements should not degrade the performance of the original software.
- New functions should not interfere with the existing functions of other software that is simultaneously in use with the original and enhanced software.
- The existing user interface and its methodology/procedures for using the original software should be maintained as much as possible, with variations from the original procedures to be thoroughly documented.

Since the AirMobile client software is a released product, it shall be background tested as a result of testing ArmorMail with the cc:Mail Mobile program. However, since the AirMobile X.25 server software is still a Beta release, it will be more thoroughly tested, first using cc:Mail Mobile alone, then using ArmorMail with cc:Mail Mobile.

Detailed procedures are described in section 5.

4.1. Baseline Establishment

In order to set a baseline for encryption testing, e-mail will first be delivered using non-encrypting systems. Once a baseline is established, secure wireless e-mail testing will take place. This will be performed using both cc:Mail and Microsoft Mail.

4.1.1. Lotus cc:Mail

Some types of messages that will be transmitted using cc:Mail are:

- Standard message traffic between users on the LAN.
- Messages that include attachments of various sizes.
- Messages that include logging, return receipts, and cc: to the sender.

4.1.2. Ardis and AirMobile Wireless for Lotus cc:Mail Mobile

In addition to using the standard cc:Mail, the same types of messages will be delivered using cc:Mail Mobile and AirMobile wireless software over the Ardis network. Additional functions that will be tested include "Docking Mode", directory updates, and network coverage.

4.1.3. AirMobile X.25 Server

The AirMobile X.25 server software will be tested for data throughput and reliability as follows:

- One small message.
- One large message.
- Multiple small messages.
- Multiple large messages (including attachments).
- Multiple users.

4.1.4. Microsoft Mail

Some types of messages that will be transmitted using MSMail are:

- Standard message traffic between users on the LAN.
- Messages that include attachments of various sizes.
- Messages that include logging, return receipts, and cc: to the sender.

4.1.5. Microsoft Mail Remote and Microsoft Mail External

In addition to using the standard MS Mail, the same types of messages will be delivered using MSMail Remote over modems. The server will be running MSMail External which is an interface from the server modem to the mail network and post office. MSMail Remote will also be tested in network mode over the LAN.

4.2. ArmorMail

Once the baseline testing is complete, system testing of the ArmorMail encryption software will be performed. Both signed and encrypted messages will be transmitted using the following network configurations:

- Testing using the MSMail program over the LAN.
- Testing using the MSMail Remote program over a dialup link and over the LAN.
- Testing using the cc:Mail program over the LAN.
- Testing using the cc:Mail Mobile program over AirMobile using wireless modems, over a dialup link, and over the LAN. Testing with the AirMobile server shall be through the X.25 connection and using a wireless modem.

Combined testing shall consist of secure communications between all of the above software packages and systems.

Among the security tests that will be performed are:

- FORTEZZA Card tests.
- PIN Number tests.
- Tests related to the FORTEZZA.DIR file.
- Tests related to the Compromised Key List file (CKLFILE).
- Encrypted Message tests.
- Shutdown and restart tests
- Proper display of requesters, responses, and other information.

The security tests shall be performed using both the cc:Mail and MSMail software packages in wired and wireless modes.

4.2.1. ArmorMail using Microsoft Mail

All of the previous tests using MSMail shall be performed with the addition of the ArmorMail procedures listed in section 6.2.

4.2.2. ArmorMail using Microsoft Mail Remote

All of the previous tests using MSMail Remote shall be performed with the addition of the ArmorMail procedures listed in section 6.2.

4.2.3. ArmorMail using Lotus cc:Mail

All of the previous tests using cc:Mail shall be performed with the addition of the ArmorMail procedures listed in section 6.2.

4.2.4. ArmorMail using Lotus cc:Mail Mobile

All of the previous tests using cc:Mail Mobile shall be performed with the addition of the ArmorMail procedures listed in section 6.2.

5. Encryption Software Test Procedures

The following procedures test the ArmorMail encryption software. The procedures exercise functions with previously known problems to verify that they have been corrected.

FORTEZZA Card:	Procedure	Verify	Pass/Fail
No Card	Begin the program with no card inserted in the card reader. Verify that the program recognizes that there is no card.	SHH	P
Uninitialized Card	Begin the program with an uninitialized card. Verify that the program recognizes that the card is uninitialized.	SHH	P
Invalid Card	Begin the program with an invalid card. Verify that the program recognizes that the card is invalid.	SHH	P
Valid Card	Begin the program with a valid card. Verify that the program recognizes that the card is valid.	SHH	P

Table 1. - FORTEZZA Card Functional Tests

PIN Number:	Procedure	Verify	Pass/Fail
No PIN number.	Do not enter a PIN number and press ENTER. Verify that the program detects that there is no PIN number.	SHH	P
Invalid PIN number.	Enter an invalid PIN number. Verify that the program detects that the PIN number is invalid.	SHH	P
All zeros.	Enter all zeros for the PIN number and press ENTER. Verify that the program detects that the PIN number is invalid.	SHH	P
All 9's.	Enter all 9's and press ENTER. Verify that the program detects that the PIN number is invalid.	SHH	P
Valid PIN number.	Enter a valid PIN number and press ENTER. Verify that the program detects that the PIN number is valid.	SHH	P
Valid PIN number with non-numeric characters included.	Enter a valid PIN number but include some non-numeric characters. Verify that the program detects that the PIN number is invalid.	SHH	P

Table 2. - FORTEZZA PIN Number Tests

FORTEZZA.DIR file:	Procedure	Verify	Pass/Fail
NO FILE: Begin program.	Begin the program with no FORTEZZA.DIR file in the directory. Verify that the program detects that the file is missing.	SHH	P
NO FILE: Send signed message.	Send a signed message with no FORTEZZA.DIR file in the directory. Verify that the program detects that the file is missing.	SHH	P
NO FILE: Send encrypted message.	Send an encrypted message with no FORTEZZA.DIR file in the directory. Verify that the program detects that the file is missing.	SHH	P
EMPTY FILE:	Procedure	Verify	Pass/Fail
Begin program.	Begin the program with an empty FORTEZZA.DIR file in the directory. Verify that the program detects that the file is missing.	SHH	P
Send signed message.	Send a signed message with an empty FORTEZZA.DIR file in the directory. Verify that the program detects that the file is missing.	SHH	P
Send encrypted message.	Send an encrypted message with an empty FORTEZZA.DIR file in the directory. Verify that the program detects that the file is missing.	SHH	P

Table 3. - FORTEZZA.DIR File Tests

FILE CONDITIONS: Send an encrypted message for each of the following conditions in the file:	Procedure	Verify	Pass/Fail
Invalid user name.	WrongName ~CertificateName(000001\00006002.8d). Verify that an invalid user is detected.	SHH	P
Uppercase name.	MYNAME ~CertificateName(000001\00006002.8d). Verify that a valid user is detected.	SHH	F
Lowercase name.	myname ~CertificateName(000001\00006002.8d). Verify that a valid user is detected.	SHH	P
Capitalized name.	Myname ~CertificateName(000001\00006002.8d). Verify that a valid user is detected.	SHH	F

Table 3. - FORTEZZA.DIR File Tests (cont'd)

FILE CONDITIONS: Send an encrypted message for each of the following conditions in the file:	Procedure	Verify	Pass/Fail
Duplicate name with duplicate certificate directory path.	ThisName ~CertificateName(000001\00006002.8d) ThisName ~CertificateName(000001\00006002.8d). Verify that the program allows a duplicate name.	SHH	P
Different name with a duplicate certificate directory path:	HisName ~CertificateName(000001\00006002.8d) ThisName ~CertificateName(000001\00006002.8d). Verify that an invalid user is detected.	SHH	F
Duplicate name with a different certificate directory path.	ThisName ~MyCertificateName(000001\00006002.8d) ThisName ~HisCertificateName(000001\00006001.fc). Verify that the program detects that the directory path is invalid.	SHH	F

Table 4. - Certificate File Verification Tests

CKLFILE:	Procedure	Verify	Pass/Fail
No CKLFILE.	Begin the program with no CKLFILE. Verify that the program detects that the CKLFILE is missing.	SHH	P
Empty CKLFILE.	Begin the program with an empty CKLFILE. Verify that the program detects that the CKLFILE is invalid.	SHH	P
Invalid CKLFILE.	Begin the program with an invalid CKLFILE. Verify that the program detects that the CKLFILE is invalid.	SHH	P
Expired CKLFILE.	Begin the program with an expired CKLFILE. Verify that the program detects that the CKLFILE has expired.	SHH	P

Table 5. - CKLFILE Tests

Display:	Procedure	Verify	Pass/Fail
Login requester does not jump.	Verify that when starting the program, the Login requester does not jump to different parts of the screen.	SHH	P
All requesters close completely.	Verify that all requesters close completely without having to refresh the screen to remove leftover images.	SHH	F
Encrypted Messages:	Procedure	Verify	Pass/Fail
Send encrypted messages before signing.	Send encrypted messages before signing has taken place. Verify that the program detects that the user is unknown.	SHH	P
Shutdown:	Procedure	Verify	Pass/Fail
Quit the program, then restart.	Quit the program, then be able to start it again without having to leave Windows.	SHH	F

Table 6. - Miscellaneous Functional Tests

6. System Test Procedures

6.1. Unencrypted E-Mail Test Procedures

The unencrypted system test procedures are a combination of wired and wireless e-mail tests. These test combinations are detailed in the table below:

	Standard Mail	Attach-ments	cc: To Sender	Multiple Recipients	Logging	Return Receipt
cc:Mail - cc:Mail Mobile	X	X		X		X
cc:Mail Mobile - cc:Mail	X		X		X	
cc:Mail Mobile - cc:Mail Mobile	X					
MSMail - MSMail Remote	X	X		X		X
MSMail Remote - MSMail	X		X		X	
MSMail Rmt. - MSMail Rmt.	X					

Table 7. - Unencrypted E-Mail Test Matrix

The test procedures for non-encrypted mail delivery are described in the table below:

cc:Mail - cc:Mail Mobile	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
Attachments	Send a mail message with an attachment. Verify that it is received at its destination.	SHH	P
Multiple Recipients	Send a mail message to multiple recipients. Verify that they are received at their destinations.	SHH	P
Return Receipt	Send a mail message with a return receipt requested. Verify that the message is received at its destination and that the receipt is received at the source.	SHH	P
cc:Mail Mobile - cc:Mail	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
cc: To Sender	Send an unattached mail message with a copy to be sent to the sender. Verify that it is received at its destination and at the source.	SHH	P
Logging	Send an unattached mail message with logging turned on. Verify that the message is received at its destination.	SHH	P
cc:Mail Mobile - cc:Mail Mobile	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P

Table 8. - Unencrypted E-Mail Test Procedures

MSMail - MSMail Remote	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
Attachments	Send a mail message with an attachment. Verify that it is received at its destination.	SHH	P
Multiple Recipients	Send a mail message to multiple recipients. Verify that they are received at their destinations.	SHH	P
Return Receipt	Send a mail message with a return receipt requested. Verify that the message is received at its destination and that the receipt is received at the source.	SHH	P
MSMail Remote - MSMail	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
cc: To Sender	Send an unattached mail message with a copy to be sent to the sender. Verify that it is received at its destination and at the source.	SHH	P
Logging	Send an unattached mail message with logging turned on. Verify that the message is received at its destination.	SHH	P
MSMail Remote - MSMail Remote	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P

Table 8. - Unencrypted E-Mail Test Procedures (cont'd)

6.2. Encrypted E-Mail Test Procedures

The encrypted system test procedures are a combination of wired and wireless e-mail tests. These test combinations are detailed in the table below:

	Standard Mail	Attach-ments	cc: To Sender	Multiple Recipients	Logging	Return Receipt
cc:Mail - cc:Mail	X	X			X	
cc:Mail - cc:Mail Mobile	X		X	X		X
cc:Mail Mobile - cc:Mail	X		X	X		X
cc:Mail Mobile - cc:Mail Mobile	X	X			X	
MSMail - MSMail	X	X			X	
MSMail - MSMail Remote	X		X	X		X
MSMail Remote - MSMail	X		X	X		X
MSMail Rmt. - MSMail Rmt.	X	X			X	

Table 9. - Encrypted E-Mail Test Matrix

The test procedures for encrypted mail delivery are described in the table below:

cc:Mail - cc:Mail	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
Attachments	Send a mail message with an attachment. Verify that it is received at its destination.	SHH	P
Logging	Send an unattached mail message with logging turned on. Verify that the message is received at its destination.	SHH	F

Table 10. - Encrypted E-Mail Test Procedures

cc:Mail - cc:Mail Mobile	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
cc: To Sender	Send an unattached mail message with a copy to be sent to the sender. Verify that it is received at its destination and at the source.	SHH	P
Multiple Recipients	Send a mail message to multiple recipients. Verify that they are received at their destinations.	SHH	P
Return Receipt	Send a mail message with a return receipt requested. Verify that the message is received at its destination and that the receipt is received at the source.	SHH	P
cc:Mail Mobile - cc:Mail	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
cc: To Sender	Send an unattached mail message with a copy to be sent to the sender. Verify that it is received at its destination and at the source.	SHH	P
Multiple Recipients	Send a mail message to multiple recipients. Verify that they are received at their destinations.	SHH	P
Return Receipt	Send a mail message with a return receipt requested. Verify that the message is received at its destination and that the receipt is received at the source.	SHH	P

Table 10. - Encrypted E-Mail Test Procedures (cont'd)

cc:Mail Mobile - cc:Mail Mobile	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
Attachments	Send a mail message with an attachment. Verify that it is received at its destination.	SHH	P
Logging	Send an unattached mail message with logging turned on. Verify that the message is received at its destination.	SHH	P
MSMail - MSMail	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
Attachments	Send a mail message with an attachment. Verify that it is received at its destination.	SHH	P
Logging	Send an unattached mail message with logging turned on. Verify that the message is received at its destination.	SHH	P

Table 10. - Encrypted E-Mail Test Procedures (cont'd)

MSMail - MSMail Remote	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
cc: To Sender	Send an unattached mail message with a copy to be sent to the sender. Verify that it is received at its destination and at the source.	SHH	P
Multiple Recipients	Send a mail message to multiple recipients. Verify that they are received at their destinations.	SHH	P
Return Receipt	Send a mail message with a return receipt requested. Verify that the message is received at its destination and that the receipt is received at the source.	SHH	P
MSMail Remote - MSMail	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
cc: To Sender	Send an unattached mail message with a copy to be sent to the sender. Verify that it is received at its destination and at the source.	SHH	P
Multiple Recipients	Send a mail message to multiple recipients. Verify that they are received at their destinations.	SHH	P
Return Receipt	Send a mail message with a return receipt requested. Verify that the message is received at its destination and that the receipt is received at the source.	SHH	P

Table 10. - Encrypted E-Mail Test Procedures (cont'd)

MSMail Remote - MSMail Remote	Procedure	Verify	Pass/Fail
Standard Mail	Send an unattached mail message. Verify that it is received at its destination.	SHH	P
cc: To Sender	Send an unattached mail message with a copy to be sent to the sender. Verify that it is received at its destination and at the source.	SHH	P
Multiple Recipients	Send a mail message to multiple recipients. Verify that they are received at their destinations.	SHH	P
Return Receipt	Send a mail message with a return receipt requested. Verify that the message is received at its destination and that the receipt is received at the source.	SHH	P

Table 10. - Encrypted E-Mail Test Procedures (cont'd)

APPENDIX E: Problem History of LJL ArmorMail Software for Lotus cc:Mail

This paper describes the overall history of problems discovered in each release of Alpha and Beta versions of ArmorMail for Lotus cc:Mail and cc:Mail Mobile encryption software. The problems are listed in chronological order, by date and by software version number.

6/1/95 Beta 1.1 Fortezza 2.75

This version would not work with Locus cc:Mail version 2.2. It would not decrypt and would not allow the use of icons for creating and sending messages.

When tested with version 2.0, it was able to use the TESSERA card, but the window would occasionally freeze.

The LOGIN requester would initially appear in one position on the screen, then jump to the center of the screen.

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program."

When trying to create a message, the message area would be blank and could not be used. The busy pointer (hourglass) would be active. There would be no address list from which to get user names. The "To:" and "cc:" indicators were duplicated in the upper left corner.

Attachments could not be sent as they would not be encrypted.

6/5/95 Alpha 1.1 Fortezza 2.77

This version would not work with Locus cc:Mail version 2.2. It would not decrypt and would not allow the use of icons for creating and sending messages.

When tested with version 2.0, it was able to use the TESSERA card, but the window would occasionally freeze.

The LOGIN requester would initially appear in one position on the screen, then jump to the center of the screen.

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program." It would then give the message: "Application Execution Error" and would crash Windows.

When ArmorMail was active, it could not be disabled by selecting the pulldown menu, "Release Armor." It was not enabled.

When trying to create a message, the message area would be blank and could not be used. The busy pointer (hourglass) would be active. There would be no address list from which to get user names. The "To:" and "cc:" indicators were duplicated in the upper left corner.

Attachments could not be sent as they would not be encrypted.

6/26/95 Alpha Fortezza 2.81

This version would work with Locus cc:Mail version 2.2.

This version not allow the use of icons for creating and sending messages.

This version was able to use the TESSERA card, but the window would not refresh properly.

The LOGIN requester would initially appear in one position on the screen, then jump to the center of the screen.

The message area was working properly but still there was no address list from which to get user names.

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program."

When using cc:Mail Mobile and ArmorMail was active, it could not be disabled by selecting the pulldown menu, "Release Armor" if a new message was opened then canceled.

Attachments could not be sent as they would not be encrypted.

7/6/95 Beta Fortezza 2.81

This version not allow the use of icons for creating and sending messages.

In this version only the FORTEZZA card was supported.

The LOGIN requester would initially appear in one position on the screen, then jump to the center of the screen.

The message area was working properly but still there was no address list from which to get user names.

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program."

When using cc:Mail Mobile and ArmorMail was active, it could not be disabled by selecting the pulldown menu, "Release Armor" if a new message was opened then canceled. This could be corrected by closing then opening the INBOX.

Attachments could not be sent as they would not be encrypted.

When a Signed message was received, the Sign Verification message box would be blank.

9/5/95 Beta 1/26 Fortezza 2.91

This version not allow the use of icons for creating and sending messages.

On startup the message: " Fatal. cc:Armor doesn't Currently support cc:Mobile", but then the LOGIN requester would appear.

The LOGIN requester would initially appear in one position on the screen, then jump to the center of the screen.

The message area and the address list were working properly .

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program." After clicking on the "OK" button, it was then possible to start the program.

When using cc:Mail Mobile and ArmorMail was active, it could not be disabled by selecting the pulldown menu, "Release Armor" if a new message was opened then canceled. This could be corrected by closing then opening the INBOX.

When trying to send a message, the response was: "CC_ARMOR An error occurred in your application. If you choose Ignore, you should save your work in a new file. If you choose Close, your application will terminate." Choosing "Close" causes: "Application error. CC_ARMOR caused a General Protection Fault in module LJL_FORT.DLL at 0007:0C4D", then the program crashes to DOS.

9/6/95 Beta 1/26 Fortezza 2.91

This version not allow the use of icons for creating and sending messages.

On startup the message: " Fatal. cc:Armor doesn't Currently support cc:Mobile", but then the LOGIN requester would appear.

The LOGIN requester would initially appear in one position on the screen, then jump to the center of the screen.

The message area and the address list were working properly .

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program." After clicking on the "OK" button, it was then possible to start the program.

When adding an attachment, the attached file was deleted from the disk instead of being copied to the mail message.

When using cc:Mail Mobile and ArmorMail was active, it could not be disabled by selecting the pulldown menu, "Release Armor" if a new message was opened then canceled. This could be corrected by closing then opening the INBOX.

When trying to send a message, the response was: "CC_ARMOR An error occurred in your application. If you choose Ignore, you should save your work in a new file. If you choose Close, your application will terminate." Choosing "Close" causes: "Application error. CC_ARMOR caused a General Protection Fault in module LJL_FORT.DLL at 0007:0C4D", then the program crashes to DOS.

9/8/95 Beta 1.31 Fortezza 2.92

This version not allow the use of icons for creating and sending messages.

The LOGIN requester would initially appear in one position on the screen, then jump to the center of the screen.

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program." After clicking on the "OK" button, it was then possible to start the program.

When using cc:Mail Mobile and ArmorMail was active, it could not be disabled by selecting the pulldown menu, "Release Armor" if a new message was opened then canceled. This could be corrected by closing then opening the INBOX.

When a message was created and sent, the message was sent to the OUTBOX correctly, but the mouse pointer would freeze in busy mode and it was impossible to click on anything.

When selecting an attachment from a file list, the standard cc:Mail would allow typing "*.xxx" and pressing Return, and all files with that suffix would be displayed. In ArmorMail, the file requester would simply close. Once the file was selected directly, that filename would appear in

the message. If the window were then resized, the filename would be replace by the standard icon. Clicking on the icon would make the filename reappear.

Attachments could be copied to the mail message correctly and the files would not be deleted.

In LAN mode, when sending a self-addressed Signed message the message transfer would work. When sending a Signed message self-addressed and to another person, the program would display, "VIM Error".

9/13/95 Beta 1.34 Fortezza 2.92

This version not allow the use of icons for creating and sending messages.

The LOGIN requester would initially appear in one position on the screen, then jump to the center of the screen.

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program." After clicking on the "OK" button, it was then possible to start the program.

When using cc:Mail Mobile and ArmorMail was active, it could not be disabled by selecting the pulldown menu, "Release Armor" if a new message was opened then canceled. This could be corrected by closing then opening the INBOX.

When selecting an attachment from a file list, ArmorMail would now allow typing "*.xxx" and pressing Return, and all files with that suffix would be displayed.

If the window were then resized, the filename would be replace by the standard icon. Clicking on the icon would make the filename reappear.

When the program is started, the PIN requester is displayed. If the PIN requester is canceled and then "FORTEZZA" is selected from the pulldown menu and canceled again, the PIN requester does not disappear completely (refresh problem).

A CKLFILE requester is displayed: "CKL FILE Has Expired You may be communicating with bad users! Do your wish to continue?" (bad grammar included). Select "No", then request FORTEZZA from the pulldown menu. The program dies with the message: CCMAIL caused a General Protection Fault in module OVERIDER.DLL at 0002:19D5". Exit and try to quit Windows. The message: "CC_ARMOR caused a General Protection Fault in module LJL_FORT.DLL at 0002:4E58" is displayed. Windows will now close.

The message, "Certificate Revoked" is displayed even though the certificate is good.

9/25/95 Beta 1.34 Fortezza 2.92

This version allows the use of an icon for creating messages but the pulldown menu must be used for sending messages.

The LOGIN requester would initially appear in one position on the screen, then jump to the center of the screen.

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program." After clicking on the "OK" button, it was then possible to start the program.

When using cc:Mail Mobile and ArmorMail was active, it could not be disabled by selecting the pulldown menu, "Release Armor" if a new message was opened then canceled. This could be corrected by closing then opening the INBOX.

If the window were then resized, the filename would be replace by the standard icon. Clicking on the icon would make the filename reappear.

The PIN requester refresh problem has been corrected.

The program is intermittently ignoring the attached files when sending messages in encrypted mode.

With the Spyrus cards, when the PIN number is entered the program responds with a window banner, "Fortezza Error Report", and the message, "FORTEZZA ERROR: CKL Check Returns: The CKL file failed verification." When OK or CANCEL is selected, the window closes but part of it is still showing (like the earlier PIN requester refresh problem).

10/26/95 Beta 1.38FWF Fortezza 2.95

Initially an "Invalid Login" message appears indicating "One or More Parameters are Incorrect." After clicking on the "OK" button, a requester would be displayed and it was then possible to start the program.

When the PIN requester was displayed and the PIN number was entered, when pressing RETURN, the computer beeped and did not accept the entry. (Occurred once.)

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program." After clicking on the "OK" button, it was then possible to start the program.

If MSG. 1 was decrypted then forwarded, the forwarding would work. If MSG. 2 is NOT decrypted then forwarded, it would include and forward the contents of MSG. 1.

This version allows the use of an icon for creating messages but the pulldown menu must be used for sending messages.

When using cc:Mail Mobile and ArmorMail was active, it could not be disabled by selecting the pulldown menu, "Release Armor" if a new message was opened then canceled. This could be corrected by closing then opening the INBOX.

If the window were then resized, the filename would be replace by the standard icon. Clicking on the icon would make the filename reappear.

The program is intermittently ignoring the attached files when sending messages in encrypted mode.

With the Spyrus cards, when the PIN number is entered the program responds with a window banner, "Fortezza Error Report", and the message, "FORTEZZA ERROR: CKL Check Returns: The CKL file failed verification." When OK or CANCEL is selected, the window closes but part of it is still showing (like the earlier PIN requester refresh problem).

12/4/95 Beta 1.41B Fortezza 2.97:cc

The "Invalid Login" message problem has been corrected.

When exiting the program, it would not allow restarting of the program. The message was, "Cannot start more than one copy of the specified program." After clicking on the "OK" button, it was then possible to start the program.

The message forwarding problem has been corrected.

This version allows the use of an icon for creating messages but the pulldown menu must be used for sending messages.

The resizing problem has been corrected.

The program is now correctly including the attached files when sending messages in encrypted mode.

The CKL verification problem has been corrected.

1/19/96 Beta 1.41K Fortezza 2.A4

The program now loads properly using a single icon.

This version has full icon support.

When running the Mobile version of cc:Mail, the cc:Mail program will crash when trying to send a message if Signing or Encryption is enabled. This a problem with the Mobile version only (according to LJL). They know about it and should have a fix in about a week.

☆U.S. GOVERNMENT PRINTING OFFICE: 1997-509-127-47202

MISSION OF ROME LABORATORY

Mission. The mission of Rome Laboratory is to advance the science and technologies of command, control, communications and intelligence and to transition them into systems to meet customer needs. To achieve this, Rome Lab:

a. Conducts vigorous research, development and test programs in all applicable technologies;

b. Transitions technology to current and future systems to improve operational capability, readiness, and supportability;

c. Provides a full range of technical support to Air Force Material Command product centers and other Air Force organizations;

d. Promotes transfer of technology to the private sector;

e. Maintains leading edge technological expertise in the areas of surveillance, communications, command and control, intelligence, reliability science, electro-magnetic technology, photonics, signal processing, and computational science.

The thrust areas of technical competence include: Surveillance, Communications, Command and Control, Intelligence, Signal Processing, Computer Science and Technology, Electromagnetic Technology, Photonics and Reliability Sciences.